Biennial Report to Congress on Improving Industrial Security

U.S. Department of Defense

September 1, 2009

Biennial Report to Congress on Improving Industrial Security

This report complies with Section 845 of the National Defense Authorization Act (NDAA) for Fiscal Year 2009 (Public Law 110-417), which requires the Secretary of Defense to report biennially to the congressional defense committees on expenditures and activities of the Department of Defense (DoD) in carrying out the requirements of this section (i.e., Defense Industrial Security).

In accordance with a clerical amendment, this first biennial report addresses the period from the date of the enactment of the NDAA to the issuance of such report. Unless otherwise stated, all information contained in this report covers the reporting period of October 1, 2008, to May 31, 2009; with all information current as of May 31, 2009. The May 31st cutoff was essential to allow sufficient time to compile and analyze data.

Topic I: The workforce responsible for carrying out the requirements of this section, including the number and experience of such workforce; training in the performance of industrial security functions; performance metrics; and resulting assessment of overall quality.

The below chart reflects DSS Fiscal Year 2009 authorized workforce for providing direct support to the oversight and administration of the National Industrial Security Program (NISP) and shows actual manning against the authorized billets.

Defense Security Service	**Authorized FY 09**	**Actual (as of May 31, 2009)**
Industrial Security Field Operations (ISFO)	348	312
Industrial Security Policy and Programs (ISPP)	25	18
Defense Industrial Security Clearance Office (DISCO)	125	109
DSS Counterintelligence Office (CI)	35	35
TOTALS	533	474

ISFO is an organizational element of DSS that works with cleared companies across the United States to ensure the protection of classified information. ISFO is comprised of Industrial Security Representatives (ISRs), who are general security specialists, as well as Information Systems Security Professionals (ISSPs), who are technical experts who accredit industry information systems to process classified information. ISFO also includes a headquarters element that oversees field personnel.

ISPP is another organizational element of DSS. This office adjudicates Foreign Ownership, Control or Influence (FOCI), administers international programs, and provides industrial and personnel security policy guidance to industry.

DISCO adjudicates Personnel Security Investigations for personnel of cleared companies.

The DSS CI works in concert with ISFO to identify threats to cleared industry and to inform cleared companies of these threats to allow for the application of effective countermeasures.

The DSS workforce is in a state of transition with a wide-range of experience and expertise. Approximately one-third of its workforce is eligible for retirement, many of whom are in the field. These employees have extensive knowledge and are well-trained and well-versed in the NISP. DSS is also hiring new personnel to not only replace its retiring workforce, but to fill 137 new positions authorized. The challenge for DSS is effective succession planning to help transition this knowledge base without losing critical skills. DSS also recognizes the challenge of ensuring that new employees are trained and properly resourced to fulfill their new missions.

All new ISRs assigned at DSS participate in a formal mentoring program with more experienced personnel. This is followed by an intensive four-week Industrial Security Specialist Course, offered in residence at the DSS Academy (DSSA). In addition to the instructors, a number of field personnel and experts within DSS serve as class counselors and provide real-world examples throughout the course. Specialized training in Counterintelligence, Information Systems, Business Structures and other areas is available for individuals serving in those positions.

DSS is constantly evaluating its training and assessing the quality of its workforce and is confident it has a high quality, high performing workforce. The following training initiatives were undertaken at the DSSA in the past year to support the DSS workforce responsible for the oversight of the NISP:

- Hosted and facilitated focus groups to conduct job analyses of the following DSS positions: ISR; FOCI/International Specialist; ISSP; and Field Office Chief. These focus group meetings are designed to develop skills and competencies that reflect both work and worker-oriented requirements associated with these positions. Results from the skills analyses will be used to conduct a training needs assessment, development of a comprehensive training curriculum, and ultimately development of a certification program.

- Launched a New Supervisor's Course for the DSS workforce to explain the "nuts and bolts" of hiring and human resources, performance management, delegation, motivation, feedback and coaching, managing diversity and time management.

- Launched a new course, "Business Structures in the National Industrial Security Program (NISP)." The course provides fundamental information about how companies are commonly organized and how the organization of a company relates to the granting of a facility clearance. This course has received a number of awards for its content and presentation.

- Beta tested a new web-based course "Safeguarding Classified Information in the NISP." This course will become part of the online curriculum of courses supporting the NISP. The target audience for this course includes Facility Security Officers (FSOs) and DoD Contractors, DSS ISRs, DoD Security Specialists, and Security Specialists from other U.S. Government agencies who interact with NISP cleared companies. This new online course will allow NISP training to be available "anytime/anywhere" and eliminates the traveling costs associated with classroom training.

- Launched the new web-based course "Visits and Meetings in the National Industrial Security Program." The target audience includes FSOs and security staff of cleared facilities, DSS ISRs, DoD Security Specialists and Security Specialists from other U.S. Government agencies that exchange visitors with NISP cleared companies.

DoD conducted a study of DSS in the spring/summer of 2008 which culminated in the Department agreeing to strengthen and refocus DSS to meet 21st century industrial security and counterintelligence needs. As a result, DSS undertook a number of initiatives in the past year to improve its oversight of the NISP. These initiatives are outlined in Appendix B.

DSS has established metrics to measure its performance in the oversight and administration of the NISP. The metrics are designed to let DSS know how it is using its resources and to trouble shoot problem areas. To gather this information, DSS has developed a method of data calls across the agency to collect and compile the information. The following are examples of the metrics and all information is current as of May 31, 2009 (NOTE: "days" refers to calendar days):

- Percent of initial facility clearance determinations completed within an average of 25 days (97.5%).

- Percent of initial facility clearance determinations completed within an average of 30 days (99.5%).
- Percentage of scheduled security inspections completed (49%).
- Average information system accreditation cycle time (37.125 days). (NOTE: This refers to the time it takes to accredit information systems in cleared facilities to process classified information.)
- Serious security deficiency rate for inspections completed during the period February 1, 2009, to May 31, 2009 (14%). A "serious" security deficiency is substantive in nature and could result in loss or compromise of classified information. (NOTE: No tracking system was available to capture this data prior to February 2009.)

Topic II: A description of funds authorized, appropriated, or reprogrammed to carry out the requirements of this section, the budget execution of such funds, and the adequacy of budgets provided for performing such purpose.

DoD has funded $61.9 million for Fiscal Year 2009 requirements and $76.6 million for Fiscal Year 2010 to perform NISP oversight. Based on current projections and requirements known at the time of this report, this funding is expected to be sufficient:

DSS Funding for Major Programs
Fiscal Years 2009 and 2010
(in millions of dollars)

	FY09	FY10
NISP[1]	61.9	76.6
CI	4.6	14.4
PSI-I[2]	224.9	230.6
PSC[3]	32.4	27.4

Budget execution for Fiscal Year 2009 is on target.

[1] NISP funding includes funding for both the Industrial Security Field Operations and Industrial Security Policy and Programs Offices.

[2] PSI-I funding refers to direct reimbursable expenditures to the Office of Personnel Management to conduct investigations for individuals cleared under the National Industrial Security Program. DSS reimburses OPM for these expenses on behalf of the Department of Defense and 23 other Federal Agencies.

[3] PSC funding refers to labor and other operational costs associated with the oversight of the Personnel Security Clearance process as well as the Defense Industrial Security Clearance Office. Beginning in FY2010, PSC is aligned with NISP, Industrial Security Policy.

Topic III: Statistics on the number of contractors handling classified information of the Department of Defense, and the percentage of such contractors who are subject to foreign ownership, control or influence.

All information is current as of May 31, 2009.

- 12,753 facilities cleared under the NISP.

- 664 cleared facilities with a current FOCI mitigation instrument in place. Based on the total cleared population, 5.2% of cleared facilities are cleared under the auspices of a FOCI mitigation agreement.

- 33 companies in various stages of the FOCI mitigation process without current agreements in place. The number of companies in process varies as new cases are opened and resolved. The average number of days to render a decision on the appropriate method of FOCI mitigation is 219 days. This processing time is down 9% from 239 days a year ago.

- During the reporting period, the FOCI case backlog, defined as those cases open for over 120 days, decreased 37% from 88 cases to 56 cases. The 56 backlogged cases include the 33 new cases, which are not yet mitigated, as well as 22 cases in process for renewals and changes of existing mitigation agreements.

- 1,058,873 persons, total active, cleared employee population within the NISP.

Topic IV: Statistics on the number of violations identified, enforcement actions taken, and the percentage of such violations occurring at facilities of contractors subject to foreign ownership, control, or influence.

DSS ISRs separate violations of National Industrial Security Operating Manual (NISPOM) requirements (hereafter referred to as deficiencies) found during inspections into two categories: Serious deficiencies and administrative deficiencies. Serious deficiencies are all substantive deficiencies that could result in loss or compromise of classified information. Examples include process or system failures, such as processing classified information on a non-accredited information system, and transmitting classified information over unsecured lines.

Administrative deficiencies are those conditions that do not place classified information at risk to loss or compromise. Some examples include incomplete visitor logs, lack of signatures on briefing statements, and the absence of initials on audit trail review checks. Available data on administrative deficiencies also includes those deficiencies corrected during the conduct of the inspection (i.e., corrected on the spot). All deficiencies noted by DSS during inspections will refer to the applicable paragraph in the NISPOM, NISPOM Supplement, or DoD Overprint to the NISPOM Supplement and include a recommended corrective action. These are policy documents that guide the contractors cleared under the NISP and DSS oversight.

The most common types of serious deficiencies found during the reporting period were:

- Failure to initiate a preliminary inquiry upon notification of a report of loss, compromise, or suspected compromise of classified information.
- Failure to appropriately mark classified information and material.
- Failure to change safe combinations to closed areas/containers when employees having access were terminated.
- Operating an information system that is or will process classified information without appropriate approval.
- Retaining classified information from an expired contract beyond the authorized two-year retention period without obtaining written retention authority from the government contracting activity.

The below chart reflects data captured by DSS from October 1, 2008, through May 31, 2009.

Summary of DSS Security Inspections of Cleared Facilities
October 1, 2008, to May 31, 2009

	All cleared facilities	**Facilities with FOCI mitigation**
Inspection Summary		
Security inspections conducted at cleared facilities	**5,622**	**311**
Total enforcement actions taken	**49**	**8**
Marginal security ratings	*10*	*0*
Unsatisfactory security ratings	*22*	*8*
Facility invalidations	*17*	*0*
Inspection Summary – Deficiencies (February 1, 2009--May 31, 2009)*		
Security inspections conducted at cleared facilities*	**2,909**	**155**
Security inspections which identified deficiencies*	1,571 (54%)	101 (65%)
Total security deficiencies identified during inspections*	**4,986**	**406**
*Count of administrative deficiencies**	*4,621*	*355*
*Count of serious deficiencies**	*365*	*51*

**Note: No system was in place to track deficiencies prior to February 1, 2009. As such, inspection items relating to deficiencies are for the time period of February 1, 2009 – May 31, 2009.*

BACKGROUND

Once a facility is cleared under the NISP, DSS has oversight authority to evaluate the security operations of the organization. At the completion of every security inspection, DSS assigns a security rating. The security ratings are defined as:

- The “Superior” security rating is reserved for cleared facilities that have consistently and fully implemented the requirements of the NISPOM in an effective fashion resulting in a security posture of the highest caliber compared with other cleared facilities of similar size and complexity. A cleared facility assigned a rating of “Superior” must have documented and implemented procedures that heighten the security awareness of company employees and must foster a spirit of cooperation within the security community. This rating also requires that a sustained high level of management support must be present for the security program.

- The “Commendable” security rating is assigned to cleared facilities that have fully implemented the requirements of the NISPOM in an effective fashion, resulting in an exemplary security posture compared with other cleared facilities of similar size and complexity. This rating denotes a security program with strong management support, the absence of any serious security issues, and only minor administrative findings.

- The “Satisfactory” security rating is the most common rating and denotes that a cleared facility’s security program is in general conformity with the basic requirements of the NISPOM. This rating can be assigned even if there were findings requiring corrective action in one or more of the security program elements within the cleared facility’s overall security program. Depending on the circumstances, a satisfactory rating can be assigned even if there were isolated serious findings during the security review.

- The “Marginal” security rating is assigned when a cleared facility’s security program is not in general conformity with the basic requirements of the NISPOM. This rating signifies a serious finding in one or more security program areas that could contribute to the eventual compromise of classified information if left uncorrected.

- The “Unsatisfactory” security rating is the most serious security rating. An unsatisfactory rating is assigned when circumstances and conditions indicate that the cleared facility has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified information in its possession or to which it has access. This rating is appropriate when the security review results indicate that the cleared facility can no longer credibly demonstrate that it can be depended upon to preclude the disclosure of classified information to unauthorized persons.

DSS will conduct a compliance inspection to identify and assess the corrective actions taken by the cleared company at facilities that receive a Marginal or Unsatisfactory security rating. A compliance inspection is generally defined as an enforcement action. The compliance inspection is completed within 120 days after the completion of a security inspection that led to the rating of “Marginal” and 60 calendar days after the completion of a security inspection that led to a rating of “Unsatisfactory.”

DSS also has the authority to invalidate or revoke a facility clearance as further enforcement actions. These actions may be taken as a result of a security inspection, compliance inspection, or if DSS becomes aware of information or actions by the cleared company which affect its ability to protect classified information. Invalidation of a facility clearance is an interim measure taken by DSS to allow the cleared company to correct the circumstances that negate the integrity of the cleared company’s security program. Invalidation allows the facility to continue to perform on existing classified work with the concurrence of their government contracting activities, but prohibits the facility from bidding on or accepting new work. When invalidating a facility clearance, DSS will set a specific deadline for corrective actions to be taken, and follows up to determine if revalidation or revocation of the facility clearance is necessary.

Revocation of a facility clearance is the most severe enforcement action DSS can take against a facility. Revocation of a facility clearance terminates a cleared company's facility security clearance rendering them ineligible to perform on or access classified information. DSS coordinates revocation decisions with the firm's government contracting activities.

Topic V: An assessment of whether major contractors implementing the program have adequate enforcement programs and have trained their employees adequately in the requirements of the program.

Of the facilities inspected by DSS during the reporting period (October 1, 2008, through May 31, 2009), DSS rated 99.4 % Satisfactory or better, indicating that the overwhelming majority of facilities cleared under the NISP are effectively protecting classified information. In order to achieve a Satisfactory security inspection rating, contractors must have at least adequate security enforcement and training programs.

DSS does not identify the relative size of cleared business organizations, large companies may have one hundred or more cleared facilities throughout the country, and there is no existing definition within DoD as to what constitutes a "major" contractor. Therefore, the data in this report are consolidated for all facilities cleared under the NISP.

A good relationship between DSS and industry depends upon cooperation and partnership on one end and strong enforcement and oversight on the other. The DSS workforce is expected to be professional in all dealings with industry, and DSS wants industry to be successful in their security programs.

The determination of whether or not a facility is implementing the NISP effectively is demonstrated in the establishment of a security program, which consistently and fully implements the requirements of the program in an effective fashion. Achieving a satisfactory rating or higher, requires a sustained high level of management support for the security program. For instance, the following are examples of facility behavior DSS considers in making these determinations:

- Demonstrated support and cooperation with the FSO.

- Personal involvement in facility security education and awareness programs.

- Absence of any serious security violations that impact integrity of security systems in place.

- Effective security staff that conducts thorough administrative inquires with prompt reporting, quality investigations and implementation of appropriate corrective actions when violations are discovered.

To better direct its resources, DSS continues to refine its threat mitigation strategy and methodology to prioritize inspections to better incorporate assessments of counterintelligence threats to the cleared U.S. companies. The goal is a coordinated, integrated visit from DSS to the right facility, at the right time with appropriate resources resulting in a more effective, meaningful inspection.

DSS has established an inspection methodology that applies an updated threat mitigation strategy and methodology to prioritize inspections. This prioritization is based on quantitative risk management factors and serves as the agency's primary assessment of risk as it relates to the overall foreign threat to key technologies within cleared companies. This ensures that the most important or highest risk facilities receive the greatest scrutiny and are expected to have the highest level security programs.

Topic VI: Trend data on attempts to compromise classified information disclosed to contractors of the Department of Defense to the extent that such data are available.

The DSS CI produces a report entitled: "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry." This DSS report is based on an analysis of Suspicious Contact Reports received from cleared companies and identifies the most frequently targeted U.S. technologies, reflects the most common collection methods utilized, identifies entities attempting the collection, and identifies the regions where these collection efforts originate.

The most recent unclassified version of this report is attached. The classified version is available upon request.

The unclassified version can also be found on the DSS website at: www.dss.mil.

PL 110-417 BIENNIAL REPORT ON IMPROVING INDUSTRIAL SECURITY

‘‘(f) BIENNIAL REPORT.—The Secretary shall report biennially to the congressional defense committees on expenditures and activities of the Department of Defense in carrying out the requirements of this section. The Secretary shall submit the report at or about the same time that the President’s budget is submitted pursuant to section 1105(a) of title 31, United States Code, in odd numbered years. The report shall be in an unclassified form (with a classified annex if necessary) and shall cover the activities of the Department of Defense in the preceding two fiscal years, including the following:

‘‘(1) The workforce responsible for carrying out the requirements of this section, including the number and experience of such workforce; training in the performance of industrial security functions; performance metrics; and resulting assessment of overall quality.

‘‘(2) A description of funds authorized, appropriated, or reprogrammed to carry out the requirements of this section, the budget execution of such funds, and the adequacy of budgets provided for performing such purpose.

‘‘(3) Statistics on the number of contractors handling classified information of the Department of Defense, and the percentage of such contractors who are subject to foreign ownership, control, or influence.

‘‘(4) Statistics on the number of violations identified, enforcement actions taken, and the percentage of such violations occurring at facilities of contractors subject to foreign ownership, control, or influence.

‘‘(5) An assessment of whether major contractors implementing the program have adequate enforcement programs and have trained their employees adequately in the requirements of the program.

‘‘(6) Trend data on attempts to compromise classified information disclosed to contractors of the Department of Defense to the extent that such data are available.’’

APPENDIX A - TRAINING

The following information is offered regarding the quality of training offered by DSS. The Council of Occupational Education (COE) conducted a team visit to DSSA to reaffirm the Academy's national accreditation in December 2008.

The COE is a national accrediting agency that is committed to assuring quality and integrity in career and workforce development. Accreditation is a status granted to an educational institution or program that has been found to meet or exceed stated criteria of educational quality. The purpose of accreditation is to assure the quality of the institution and to assist in the improvement of the institution or program.

The COE team determined that DSSA was in full compliance with all 11 standards of accreditation and the conditions of accreditation. DSSA was granted national re-accreditation by the COE Commission in February 2009. As a result, DSSA is accredited through 2015, and will conduct yearly self-studies mandated and reviewed by the COE commission.

DSSA offers 25 on-line and instructor led courses related to industrial security functions. The data below provides detailed course information and reflects that DSS personnel with Industrial Security Program oversight responsibilities participated in and completed 1,084 training courses and industry personnel participated in and completed 8,155 training courses from October 1, 2008, to May 31, 2009.

Industrial Security Course Attendance
October 1, 2008, to May 31, 2009

Course	Description	DSS Attendees	Industry Attendees
FSO Role in the NISP	Describes the role of the FSO in the NISP.		7
Getting Started Seminar for New FSOs	Provides new FSOs with an opportunity to apply fundamental NISP requirements.	7	146
Essentials of Industrial Security Management	Covers basic NISP requirements with emphasis on cleared contractor responsibilities.	153	2,202
Protecting Secret and Confidential Documents	Focuses on NISP requirements for cleared contractor facilities with authorization to store classified information.	104	955
Introduction to	Provides an introduction to the DoD	9	56

Industrial Security	Industrial Security Program.		
Introduction to Physical Security	Provides students with a basic understanding of the theories and principles involved in the application of physical security in the protection of DoD assets.	2	54
Visits and Meetings in the NISP	Covers the rules and procedures for classified visits and meetings for cleared companies participating in the NISP.	26	213
ISFD online course	Provides step-by-step instructions on the use of the Industrial Security Facilities Database (ISFD).	5	1
JPAS/JCAVS Training for Security Professionals	Provides an overview of the Joint Personnel Adjudication System (JPAS) and a detailed explanation of its subsystem, the Joint Clearance and Access Verification System (JCAVS) used by DoD personnel security managers (PSMs) and FSOs for eligibility and investigation verification.	32	362
JPAS/JCAVS Virtual Training online course	Provides an overview of the JPAS and a detailed explanation of its subsystem, the JCAVS used extensively by DoD personnel security managers (PSMs) and FSOs for eligibility and investigation verification.	12	49
Safeguarding Classified Information in the NISP	Covers the rules and procedures for protecting classified information and material in the NISP.	19	61
Derivative Classification	Explains how to derivatively classify national security information from a classification management perspective.	40	172
Transmission and Transportation for Industry	Examines the requirements and methods for transmitting or transporting classified information and other classified material in accordance with NISP.	37	128
Marking Classified Information	Examines the requirements and methods for marking classified documents and other classified material.	130	796
Security Awareness For Educators (SAFE)	Addresses how to create an effective security awareness and education program and identifies solutions for overcoming the various challenges surrounding this	19	91

	responsibility.		
SAP Orientation	Introduces students to DoD Special Access Programs (SAPs).	33	288
NISPOM Chapter 8 Security Requirements	Introduces the security requirements for safeguarding classified information processed and stored in information systems at cleared company facilities.	76	724
NISPOM Chapter 8 Security Implementation	Teaches the basics of security for Local Area Networks and practices implementation of the security requirements described in Chapter 8 of the NISPOM.	17	203
Information System Security Basics	Introduces the basics of information system security.	148	1,514
Business Structures in the NISP	Covers the most common business structures ISRs encounter when processing a company for a facility clearance.	90	133
Industrial Security Mentoring Program	Introduces new DSS ISRs to the Industrial Security Program.	29	NA
Industrial Security Specialist Course	Trains new DSS ISRs to perform basic responsibilities including initial clearance and recurring inspections of non-complex cleared facilities approved to store classified material under the NISP.	56	NA

APPENDIX B - OVERALL PROGRAM ACCOMPLISHMENTS

During Fiscal Year 2008, the Secretary of Defense directed, and the Under Secretary of Defense for Intelligence convened, an outside panel of experts to examine the four mission areas of DSS (industrial security, education and training, personnel security clearances office, and information technology). As a result of this study, DoD has initiated steps to strengthen and refocus DSS to meet 21st century industrial security and CI needs. Towards this end, DSS will enhance its oversight under the NISP to include an increased focus on CI and security education.

- Completed a reorganization of the DSS Headquarters Industrial Security Program. The new organization allows for increased emphasis and support to the Headquarters, Field and Counterintelligence missions and enhances transparency at the senior management level.

- Completed a reorganization of the DSS field structure to ensure integration of Counterintelligence, Information Technology Security, and Industrial Security generalists at both the regional and Headquarters level.

- Established a Facilities of Interest List (FIL) that defines a risk-based approach to supporting inspections and allows the agency to move from a subjective approach, to one that is proactive, integrated, and objective. DSS uses the FIL to determine the risk to a facility, to prioritize its workload based on the risk, and to tailor inspections to the risk.

- Established DSS cross-regional inspection teams for complex cleared facilities. This approach aids the professional development of the DSS workforce by exposing personnel to facilities and personnel that they would not necessarily have the opportunity to work with in their own geographic regions.

- Created a new senior Program Integration position at DSS Headquarters to develop a formal Quality Assurance Program in Field Operations.

- Created a Senior FOCI Oversight Manager position to improve oversight of cleared companies under FOCI mitigation.

- Established enhanced oversight and inspection process for firms under FOCI.

- Realigned the FOCI workload to provide field level adjudication on minor FOCI mitigation issues.

- Developed more robust FOCI analytical capabilities to address issues created by globalization, such as increased investment by Sovereign Wealth funds, and other investment tools where the actual investor is unknown.

- Increased the number of FOCI action officers at DSS Headquarters.

- Moved from classroom based training to more web-based training. This allows DSSA to deliver training to those who need it, when and where they need it.

- Increased the number of course offerings available at DSSA and developed new training products and services.